UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,099	04/09/2001	Binyamin Pinkas	704-X00-47US	2969

7590 08/10/2004

EXAMINER
SON, LINH L D

ART UNIT	PAPER NUMBER
2135	3

DATE MAILED: 08/10/2004

Martin Fleit
Fleit Kain Gibbons Gutman & Bongini
520 Brickell Key Drive
Miami, FL 33131

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/807,099	PINKAS ET AL.	
	Examiner	Art Unit	
	Linh Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3, 5-8, 10-11, and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Shoham (US 6285989).

As per claims 1 and 2, Shoham discloses the "Universal On-Line Trading Market Design and Deployment System" invention, which includes a method for preserving the integrity of a negotiation (Col 11 lines 1-20) comprising the steps of: a) providing an architecture which includes a center A (Col 5 lines 20-65), and a plurality of users B.sub.I, B.sub.2 to B.sub.n (Col 14 lines 5-16), b) generating for each user B.sub.i an input X.sub.i (Col 14 lines 45-50), c) inputting each user's input X.sub.i to the center A (Col 10 lines 45-65 and Col 5 lines 20-27), d) computing and publishing a function F (X.sub.1,X.sub.2 to X.sub.n) by the center A based on the input messages it receives (Col 14 line 62 to Col 15 line 8), e) each user B.sub.i (1<= i<= n) communicating with the center A exclusively, and publishing by center A additional information which let each of the users verify that

F was computed correctly, and preventing a coalition of any one subset of the users from learning (i) anything which cannot be computed just from the output of the function, F(X.sub.1 to X.sub.n), and from their own inputs, and (ii) information about the inputs of other users (Col 11 lines 1-20, Col 13 lines 14-63, and Col 16 lines 42-55).

As per claim 3, the method according to any one of claims 1, for computing the output of a sealed bid auction (Col 1 lines 38-42), where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount to be paid, and wherein the center only makes disclosure to the winning bidder, while all other bidders being able to verify that the auction was computed correctly, but do not learn any other information (Col 14 line 62 to Col 15 line 8).

As per claim 5, Shoham discloses the method according claims 1, for second price auctions (Vickrey auctions), where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is greater or equal to any X.sub.i for 1 <=i <=n except for i=j1 (Col 2 lines 11-34).

As per claim 6, Shoham discloses the method according to claims 1, for k-th price auctions, where the output of F is (B.sub.j1, X.sub.j2), where X.subj1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is the k-th largest among all inputs X.sub.i for 1<=i<=n (Col 2 lines 11-34).

As per claim 7, Shoham discloses the method according to claim 1 wherein the auction is a plural auction where there is a plurality of sellers (Col 6 Table 1).

As per claim 8, Shoham discloses the method according to claim 1 wherein the auction is a generalized Vickrey auction (Col 6 Table 1).

As per claim 10, Shoham the method according to claim 1, comprising the step of; computing the output of the auction such that the users learn, in addition, some statistic of the inputs, such as, the users can learn at least one of the average of the inputs, the variance of the inputs, or how many one inputs were in a certain range (Col 15 lines 9-20).

As per claim 11, Shoham discloses the method according to claim 1, comprising the step of computing the output of the function such that only the center learns the output of the function or several of the users learn the output of the function, or all the users learn the output of the function (Col 14 line 62 to Col 15 line 8).

As per claim 16, Shoham discloses the method according to claim 1, comprising the step of computing a function by N centers, such that only if K of the N centers collude they can learn information about the parties inputs (Col 11 lines 1-20).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shoham (US 6285989).

As per claim 9, Shoham discloses the method according to claim 1. However, Shoham does not teach the step of, computing the auction such that the auctioneer wants to buy an item and each of the bidders wants to sell this item, and wherein negative values of the inputs X.sub.i are possible. Nevertheless, Shoham does teach many types of auction and method to carry out (Col 1 lines 38-67). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art that changing roles in an auction is explicitly teach and would have been obvious for one having ordinary skill in the art to implement.

Claims 4, 8, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shoham (US 6285989) in view of Ausubel (US 6026383).

As per claim 4, Shoham discloses the method according to claims 1 and the first price auctions (Col 1 lines 38-42). However, Shoham does not elaborate the first price

auctions, where the output of F is (B.sub.j, X.sub.j), where X.sub.j is greater or equal to any one X.sub.i for 1 <=i <=n. Nevertheless, Ausubel does elaborate the first price auctions completely (Col 14 lines 48-67). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the Ausubel's teaching with Shoham to ensure a great bidding process.

As per claim 8, Shoham discloses the method according to claim 1. However, Shoham does not elaborate clearly that the auction is a generalized Vickrey auction (Col 6 Table 1). Nevertheless, Ausubel does teach the Vickery auction clearly on Col 14 lines 48 to 65. Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the Ausubel's teaching with Shoham to clarify the Vickrey auction process and provide a legitimate bidding result.

As per claim 12, Shoham discloses the method according to claim 1. However, Shoham does not teach the step of, computing the output of a mechanism, in particular, for one of Groves-clark mechanisms, opinion polling and stable matching. Nevertheless Ausubel does teach the method to compute the output of the bidding session (Col 14 line 20 to Col 15 line 7). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to incorporate to provide a legitimate bidding result.

As per claims 13 and 14, Shoham discloses the method according to claim 1. However, Shoham does not discloses the steps of each user committing to the values of his input in a manner that the user cannot change it afterwards, but hiding the input value from the center, at a specific stage, the users opening their commitments to their inputs and revealing their values to the center, which then computes the value of F in a manner the each of the users can verify that the values that were used as inputs for computing F were the values that were committed to by the users. Nevertheless, Ausubel discloses the "Computer Implemented Methods and Apparatus For Auctions" invention, which teaches steps to secure the bidding value until the opening time (Col 20 lines 39-65). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the Ausubel's teaching with Shoham to create a high integrity bidding process.

Claims **15** is rejected under 35 U.S.C. 103(a) as being unpatentable over Shoham (US 6285989) in view of Naor et al, hereinafter "Naor", (US 6055508).

As per claim 15, Shoham discloses the method according to claim 1. Shoham also teach the Universal Surveillance Console (USC) which allow a third party to monitor the integrity of the operation (Col 11 lines 1-20). However, Shoham does not specifically teach the step of computing a function where the center can generate a proof that it computed the correct output of the function. Nevertheless, Naor discloses the "Method for Secure Accounting and Auditing on a Communications Network" invention, which

teaches a method of providing an auditing party to certify multiple transactions between the plurality clients and servers and able to correlate its calculation against the server calculation to proof the result (Col 6 lines 11-60). Therefore, it is obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Naor's method with Shoham to add an additional integrity check in the bidding process.

Claims 17-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al, hereinafter "Franklin", (US 6055518) in view of Noar.

As per claims 17 and 18, Franklin discloses the "Secure Auction Systems" invention, which includes a system that contains N parties (Col 3 lines 5-7), each having a private input, and a center adapted to compute a function F of said input apparatus for computing said function F in said center, comprising: a first program provided in the center that enables calculation of said function F; circuitry for publishing said function F using the program while not revealing substantially any information about said input (Col 8 line 47 to Col 10 line 2). However, Franklin does not teach a second program provided to the parties enabling each one of said parties to prove that said function F was calculated correctly. Nevertheless, Naor does teach a method of providing an auditing party to certify multiple transactions between the plurality clients and servers and able to correlate its calculation against the server calculation to proof the result (Col 6 lines 11-60). Therefore, it is obvious at the time of the invention was made for one

having ordinary skill in the art to incorporate Naor's method with Franklin to add an additional integrity check in the bidding process.

As per claim 19, Franklin and Naor disclose a system according to claim 17, wherein the second program precludes the learning of any information other than the function F was calculated correctly in a system according to claim 17, wherein the first program includes a construction of K garbled circuits for computing function F (Franklin, Col 9 line 3 to Col 10 line 2).

As per claim 20, Franklin and Noar disclose a system according to claim 17, wherein said parties are bidders in an auction, said input are bids, said center is an auctioneer, said function F is the rule by which said auction is decided, whereby the auctioneer is capable of calculating the result of said auction without revealing any information about said bids, except for the identity of the winning party from among said parties, and the amount to pay (Franklin, Col 9 lines 53-67).

As per claim 21, Franklin and Noar disclose a system according to claim 20, wherein Franklin inherently teach the function is determined utilizing a circuit of gates. The server implemented in Franklin reference includes processor to process instructions, which does have circuit of gates.

As per claim 22, Franklin and Noar disclose a system according to claim 20 wherein the second program includes the capability of utilizing the circuit of gates to independently determine and verify that the computations of the center are correct (See Claim 17 rejection). Further, Franklin inherently teach the circuit gates to determine and verify that computations of the center are correct, since the process of computation is carried out by computer which has processor.

Conclusion

1. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914.
2. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

Linh LD Son

Patent Examiner

AU 2135